Abstract of WO0101644

CN1316147A

An apparatus for securing the user's secret information transmitted from a mobile station is provided in a mobile communications system in communication with a web server through an Internet service server, wherein the data relating to the user's secret information is selected in response to the data request from the mobile station and/or web server, the selected data is enciphered in a given format, and the enciphered data is directly transmitted to the web server and/or the mobile station without any additional processing operation by the service server.

[19]中华人民共和国国家知识产权局

[51]Int. Cl⁷
H04L 12/58

[12]发明专利申请公开说明书

[21]申请号 00801224.5

[43]公开日 2001年10月3日

[11]公开号 CN 1316147A

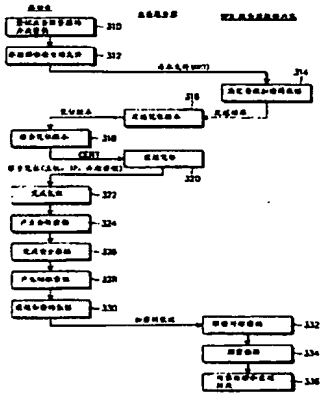
[22]申请日 2000.6.29 [21]申请号 00801224.5
[30]优先权
[32]1999.6.29 [33]KR [31]1999/25510
[86]国际申请 PCT/KR00/00689 2000.6.29
[87]国际公布 WO01/01644 英 2001.1.4
[85]进入国家阶段日期 2001.2.27
[71]申请人 三星电子株式会社
地址 韩国京畿道
[72]发明人 崔熹昌 金圣恩
[74]专利代理机构 柳沈知识产权律师事务所
代理人 马莹

权利要求书4页 说明书7页 附图页数4页

[54]发明名称 在连接到互联网的移动通信系统中用户信息的保密装置及其方法

[57]摘要

提供一种在通过一个互联网web服务器与web服务器通信的移动通信系统中,用于使从移动台发送的用户秘密信息保密的装置,其中响应于来自移动台和/或web服务器的数据请求选择涉及用户秘密信息的数据,选择的数据被以一个给定的格式加密,加密的数据被直接发送给web服务器和/或移动台,无需业务服务器任何附加的处理操作。



ISSN1008-4274

知识产权出版社出版

权 利 要 求 书

1.一种安全系统，包括至少一个移动台，一个互联网业务服务器和一个 web(网络)服务器，所述移动台可以经所述互联网向/从所述 web 服务器发送/接收数据；其特征在于，当由所述移动台或所述 web 服务器请求发送所述数据时，所述数据被以一个预定的格式加密，以传送给所述移动台或所述 web 服务器中的一个，所述加密的数据被所述移动台或所述 web 服务器中的一个解密，而不用所述互联网业务服务器进行另外的干涉。

2.如权利要求 1 所述的系统，其中所述业务服务器预先登记要被发送给所述移动台的所述 web 服务器的凭证，以便当所述移动台请求与所述 web 服务器连接时，存储在所述移动台中的先前登记的凭证被更新。

3. 如权利要求 1 所述的系统，其中按照由所述移动台或所述 web 服务器进行的发送所述数据的所述请求的类属性，有选择地加密/解密所述数据。

4. 如权利要求 3 所述的系统，其中所述数据的加密/解密是按照 Riverst-Shamier-Adleman(RSA)公共密钥算法 RSA 算法和 SEED 对称密钥算法实现的，所述 SEED 对称密钥算法是基于由韩国信息安全机构(KISA)开发的韩国数据加密标准的。

5.一种在移动互联网通信系统中的安全交易期间交换的个人信息的保密系统，包括：

一个 web 服务器，用于响应于用户的请求提供电子数据，和用于产生一个公共密钥和一个保密密钥来保密所述个人信息；

一个移动台，用了使用从所述 web 服务器接收的公共密钥，产生用于所述安全交易中的会话密钥，和用于使用所述会话密钥加密/解密所述个人信息；和

其中所述 web 服务器使用所述保密密钥解密从所述移动台接收的所述会话密钥；和

其中使用解密的会话密钥，解密由所述移动台加密的所述个人信息。

6. 如权利要求 5 所述的系统，还包括一个业务服务器，用于直接在所述移动台和所述 web 服务器之间发送所述加密的个人信息，而不用由所述业务服务器进行另外的干涉。

7. 如权利要求 5 所述的系统，其中由所述会话密钥进行的所述个人信

息的加密/解密是按照 Riverst-Shamier-Adleman(RSA)公共密钥算法 RSA 算法和 SEED 对称密钥算法实现的，所述 SEED 对称密钥算法是基于由韩国信息安全机构(KISA)开发的韩国数据加密标准的。

8.一种用于经一个业务服务器从与一个 web 服务器通信的移动通信系统的移动台发送的个人信息的保密方法，包括步骤：

接收用于从所述移动台或所述 web 服务器发送所述个人信息的请求；

以一个预定的格式可选择地加密所述个人信息，以传送给所述移动台或 web 服务器中的一个；和

由所述移动台或所述 web 服务器中的一个解密所述加密的个人信息，而不用由所述业务服务器进行任何干涉。

9. 如权利要求 8 所述的方法，还包括以下步骤，在接收发送所述个人信息的所述请求以后，从所述互联网业务服务器发送一个凭证给所述移动台。

10. 如权利要求 9 所述的方法，其中所述业务服务器预先登记要被发送给所述移动台的所述 web 服务器的凭证，以便当所述移动台请求与所述 web 服务器连接时，存储在所述移动台中的先前登记的凭证被更新。

11. 如权利要求 8 所述的方法，其中按照由所述移动台或所述 web 服务器进行的发送所述个人信息的所述请求的类属性，可选择地加密/解密所述数据。

12. 如权利要求 8 所述的方法，其中由所述移动台或所述 web 服务器进行的所述个人信息的所述加密/解密是按照 Riverst-Shamier-Adleman(RSA)公共密钥算法 RSA 算法和 SEED 对称密钥算法实现的，所述 SEED 对称密钥算法是基于由韩国信息安全机构(KISA)开发的韩国数据加密标准的。

13. 一种用于经一个业务服务器从与一个 web 服务器通信的移动通信系统的移动台发送的个人信息的保密方法，包括步骤：

响应于一个由用户进行的发送电子数据的请求，由所述 web 服务器产生一个公共密钥和一个保密密钥，所述公共密钥和所述保密密钥用于保密所述移动到和来自所述移动台的所述电子数据；

发送所述公共密钥给所述移动台；

响应于从所述 web 服务器接收的所述公共密钥，由所述移动台产生一个会话密钥，所述会话密钥用于加密/解密在所述移动台和所述 web 服务器

之间发送的所述个人信息；和

其中，所述 web 服务器使用所述保密密钥解密从所述移动台接收的所述会话密钥；和

其中，使用所述解密的会话密钥，解密由所述移动台加密的所述个人信息。

14. 如权利要求 13 所述的方法，还包括如下步骤，由所述业务服务器在所述移动台和所述 web 服务器之间发送所述加密的个人信息，而不用由所述业务服务器进行另外的干涉。

15. 如权利要求 13 所述的方法，其中采用所述会话密钥进行的所述个人信息的所述加密/解密是按照 Riverst-Shamier-Adleman(RSA)公共密钥算法 RSA 算法和 SEED 对称密钥算法实现的，所述 SEED 对称密钥算法是基于由韩国信息安全机构(KISA)开发的韩国数据加密标准的。

16.一种用于在移动互联网通信系统中发送的数据的保密方法，这种类型的通信系统具有一 web 服务器、用于和所述 web 服务器交换数据的一个移动台、和与所述移动台和所述 web 服务器通信的一个代理业务服务器，该方法包括步骤：

由所述移动台请求连接，以经所述业务服务器从所述 web 服务器接收电子数据；

响应于所述移动台的所述请求，由所述 web 服务器产生一个公共密钥和一个保密密钥；

由所述 web 服务器发送所述公共密钥给所述移动台，以在所述移动台中登记；

由所述业务服务器发送一个新的凭证给所述移动台；

由所述移动台决定在所述移动台中先前登记的凭证与从所述业务服务器接收的新的凭证是否是一样的；

如果所述新的凭证与所述先前登记的凭证是一样的，则由所述移动台使用一个由从所述 web 服务器接收的所述公共密钥产生的会话密钥来加密个人信息，和加密所述公共密钥，以产生一个对称密钥，和经所述业务服务器发送所述加密的个人信息和所述产生的对称密钥给所述 web 服务器；和

由所述 web 服务器解密从所述移动台接收的所述对称密钥，以变换回

到所述会话密钥，和使用所述变换的会话密钥和所述保密密钥，解密所述加密的个人信息。

17. 如权利要求 16 所述的方法，还包括如下步骤，如果所述新的凭证和所述先前登记的凭证是不一样的，则由所述移动台从所述业务服务器请求所述新的凭证。

18. 如权利要求 16 所述的方法，还包括步骤，由所述 web 服务器使用从所述移动台接收的所述对称密钥加密发送给所述移动台的数据；发送所述加密数据给所述移动台，和，由移动台使用先前发送给所述 web 服务器的所述对称密钥，解密从所述 web 服务器接收的所述加密的数据。

19. 如权利要求 16 所述的方法，其中采用所述会话密钥进行的所述个人信息的所述加密/解密是按照 Riverst-Shamier-Adleman(RSA)公共密钥算法 RSA 算法和 SEED 对称密钥算法实现的，所述 SEED 对称密钥算法是基于由韩国信息安全机构(KISA)开发的韩国数据加密标准的。

说　明　书

在连接到互联网的移动通信系统中用户信息的保密装置及其方法

发明背景

1. 发明领域

本发明涉及一种用于在和互联网通信的移动通信系统中的用户信息保密装置和方法。

2. 相关技术描述

在移动通信中，近来的发展已能够使用户通过互联网，使用无线电通信技术实现所谓的电子贸易。为了促进在互联网上的电子贸易，当他或她和互联 web(网络)服务器进行连接时，它提供了电子贸易的内容，最重要的事情是防止顾客的个人信息的泄漏。据此，当使用互联网时，安全系统的目的是保密用户的个人信息，以便不受欢迎的用户不会窃取用户的个人信息，例如访问 web 服务器的口令，具有相关的进行交易的口令的信用卡号等等。

在有线互联网通信中使用用于保护秘密信息的传统的安全系统一般采用安全套接字协议层(Secure Socket Layer)(SSL)，它是由美国的 Netscape Company 提议的。SSL 系统以一种已知的仅由 web 服务器可读的方式编码来自顾客的信息。然而，由于下面讨论的原因，SSL 系统不适合用于无线或移动互联网通信系统。

首先，移动台有一个限制的存储容量；在 SSL 系统中不适合于实现 web 应用。因此，传统的移动台未被设计为实现这样的 web 应用。第二，为了进行到互联网 web 服务器的无线连接，移动台首先必需和相关的互联网业务服务器连接，请求 web 内容业务。在这种情况下，为了在整个网络中适当地实现和保护个人信息，在 web 服务器和业务服务器之间的安全系统应该有与在业务服务器和移动台之间的安全系统相同的标准。然而，传统的安全系统不能在它们之间提供相同的标准。如举例说明的例子，图 1 描述了一个在传统的安全系统中提供的传统的移动通信网系统。如图示，SSL

系统被在业务服务器和 web 服务器之间采用，但是具有不同系统的无线安全系统被在移动台和业务服务器之间采用。因此，整个网络在其之间没有相同的标准。据此，先有技术的安全系统有不同的系统和标准，不适合提供用于用户个人信息的保密装置。

如上面所述，被设计来用于有线互联网通信系统的传统的安全系统不适合应用于无线互联网通信系统，因此，阻碍了使用移动通信技术通过互联网的电子贸易市场的迅速发展。

本发明概述

本发明的一个目的是，提供一种用于当使用移动互联网通信系统实现电子贸易时，使机密用户信息保密的装置和方法，其中先有技术的系统使用在有线互联网通信中采用的 SSL 系统。

本发明的另一个目的是，提供一种用于机密用户信息的保密装置和方法，其使用相同的标准，实现从移动台到 web 服务器端到端的安全性，以产生在移动台、业务服务器和 web 服务器之间的数据流。

按照本发明的一个方面，提供一个装置，用于使通过互联网业务服务器从移动台发送到 web 服务器的用户的秘密信息保密，其中，响应于来自移动台和/或 web 服务器的数据请求来选择涉及用户秘密信息的数据，选择的数据被以一个给定的格式加密，加密的数据被直接发送给 web 服务器和/或移动台，而不用业务服务器另外干涉。

本发明现在将参考附图仅通过例子更明确的描述。

附图简述

图 1 是一个示意图，用于说明具有传统的移动安全系统的传统的移动互联网通信系统；

图 2 是一个类似于图 1 的示意图，说明按照本发明的一个移动安全系统；

图 3 是一个示意图，用于说明在移动互联网通信中按照本发明的安全系统发送一个普通的 web 文件和秘密数据的过程；和

图 4 是一个流程图，用于说明按照本发明的移动互联网通信使用户信息安全的处理。

优选实施例的详细描述

在下面的描述中，为了解释的目的而不是限制，为了提供一个本发明

的准确的理解，提出特定细节，例如特定的结构、接口、技术等等。然而，对那些在本领域内的普通技术人员来说是很明显的，离开这些特定的细节，本发明可能被以另外的实施例实现。为了简洁的目的，已知装置、电路详细和方法的描述被省略，以便不会使不必要的细节使本发明的描述模糊。

为了提供一个保证的标准，声称的消息发送者事实上是真正的消息发送者，数字/电子签名可以使用各种已知的方法加密。按照本发明适合于应用的加密的算法是 Riverst-Shamier-Adleman(RSA)公共密钥算法，在目前的电子贸易安全系统中它是最广泛使用的算法。基于素数因子分解，RSA 算法既提供加密又提供电子签名(或加密密钥)。即，RSA 算法的原理是基于这样的事实，即，更容易计算两个素数“p”和“q”的乘积，但是从乘积“n”中提取出“p”和“q”是困难的，“n”是由“p”和“q”的乘积获得的。也就是说，使用两个密钥，一个是公共密钥，第二个是保密密钥，以便每当使用保密密钥加密时，仅用公共密钥解密，反之亦然。在本发明的实施例中，RSA 算法产生公共密钥和保密密钥用于加密/解密一个会话密钥。公共密钥由顾客使用加密会话密钥，然后发送加密的会话密钥送回给服务器。服务器用它的保密密钥解密会话密钥和建立与顾客的安全连接。

此外，在本发明的实施例中，用于产生会话密钥的算法使用 SEED(种子)对称密钥算法，SEED 对称密钥算法是基于韩国数据加密标准和使用由韩国信息安全机构(KISA)开发的用于公共电子贸易的 128 位块加密算法。SEED 对称算法可选的有 8、16 和 32 位数据处理，以块加密的方式解密，输入/输出短语(phrase)和输入密钥是 128 位。它也被设计来保证微分密码分析学(DC)/线性密码分析学(LC)，包括快于数据加密标准(DES)三倍的加密/解密速度。它的结构是基于 Feistel，和内部函数设计为使用由变换非线性函数获得的查寻表。在本发明中，SEED 对称密钥算法应用 12 轮，以产生会话密钥，通过它加密用户的信息数据。

按照本发明，在移动互联网通信中，移动台、互联网业务服务器和 web 服务器可以如下面描述的那样工作。

首先，移动电话被提供一个连接 web 服务器所需的本发明的安全程序，以接收公共密钥和内部产生在安全交易时使用的会话密钥。会话密钥用于加密和解密数据。按照 RSA 算法和 128 位 SEED 算法实现加密。web 服务器使用 RSA 算法产生公共密钥和保密密钥，通过发送公共密钥给移动台，

可以使移动台实现安全交易。接收的公共密钥用于产生会话密钥，以加密由移动台发送的数据，移动台使用 SEED 算法产生会话密钥。然后，web 服务器使用保密密钥解密会话密钥，用于加密由移动台发送的数据。也就是说，使用公共密钥加密的数据仅通过使用保密密钥被解密，反之亦然。因此，web 服务器使用 RSA 保密密钥解密使用 SEED 算法产生的会话密钥，按照 128 位对称密钥 SEED 的加密和解密，解密的会话密钥用于解密加密的数据。

按照本发明的实施例，当 web 服务器产生一对它自己的公共密钥和保密密钥时，在移动台和 web 服务器之间的数据处理开始。公共密钥被发送给业务服务器，然后在请求时被修正并作为凭证发送给移动台。对此，移动台已被授权使用，通过转发需要的数据，业务服务器担当在移动台和 web 服务器之间的媒介。然后，移动台存储公共密钥，以内部产生一个会话密钥来加密要发送给 web 服务器的机密数据。为了产生会话密钥，移动台加密接收的公共密钥，以产生要发送给 web 服务器的对称密钥。此后，web 服务器用它自己的保密密钥解密对称密钥。用解密的对称密钥，web 服务器解密从移动台接收的加密的数据。在相反的传送中，web 服务器使用从移动台接收的对称密钥加密要被发送给移动台的数据。移动台接下来使用先前发送给 web 服务器的对称密钥来解密从 web 服务器接收的加密的数据。在本发明的实施例中，业务服务器被作为代理服务器设置。

在移动互联网通信的每一通路上的数据格式结合附图 2 描述，其中在移动台、业务服务器和 web 服务器之间的安全系统使用本发明的移动微安全系统(MMS)。即，在移动台和 web 服务器之间采用相同的标准 MMS。由于在公共密钥被首次发送给移动台时，web 服务器的公共密钥是被以 web 服务器的保密密钥电子标记的，在移动台和移动通信网络之间的路径不会被电脑黑客使用伪造的公共密钥篡改。此外，由移动台加密的数据分组是以 128 位码的格式，以便电脑黑客不会理解原始文件的内容。进一步，当电脑黑客经互联网从移动网络移动到业务服务器时，它不会窃取数据分组。由于在移动通信网络和业务服务器之间的路径使由移动台加密的数据分组经互联网以 128 位的格式给业务服务器时，这是可以实现的，因此防止了电脑黑客窃取它的内容。

此外，通过采用本发明黑客检测系统的防火墙来保护业务服务器的内

部网络。业务服务器将加密的数据从移动台简单地传送到 web 服务器而不在其中进行任何处理操作。另外，通常采用一经其传送 128 位加密数据的专用线来连接业务服务器和 web 服务器，从而使黑客难以接入。

进一步，因为 web 服务器接收由移动台按照 128 位 SEED 算法随机产生的对称密钥，按照本发明的电脑窃取检测系统被实现。然后，web 服务器使用 RSA 保密密钥安全地解密从移动台接收的该 128 位加密数据。以这种方式，移动台的加密数据仅可以由 web 服务器解密，来自 web 服务器的加密的数据仅可由移动台解密。后者是可能的，因为 web 服务器的 SEED 对称密钥也可以相反的操作被发送给移动台。

在被发送之前，在移动台和 web 服务器之间进行通信时，在发送前，由会话密钥加密每个消息，在接收端由会话密钥解密，其中从移动台产生的会话密钥使用公共密钥被加密和作为对称密钥产生。为此，移动台被安装安全程序，用于和安全业务服务器连接。安全程序的作用是从 web 服务器接收公共密钥和接下来在内部产生会话密钥去加密个人信息，并从移动台发送给 web 服务器。也就是说，按照 RSA 加密和 128 位 SEED 对称密钥，会话密钥用于加密和解密秘密数据。

图 3 图示出不用任何加密的一个普通的 web 文件的传输，和按照本发明的被加密的秘密数据的传输。即，业务服务器在移动台和 web 服务器之间通过一个代理服务器发送一个普通 web 文件，在它们之间发送个人数据而不用任何附加的处理操作。如在图 3 中示出的，由于在无线互联网通信中可发送和处理限量的数据，按照本发明，两个不同的数据传输可操作。因此，只有需要对一个不受欢迎的第三者保密的个人/秘密数据直接在移动台和 web 服务器之间发送。

按照本发明的实施例，用图 4 描述当移动台试图和 web 服务器连接时用户信息的保密过程，其中在步骤 310 移动台登记业务服务器接收的公共密钥，它是硬敷(hard-coated)在移动台的 web 浏览器上。业务服务器伴随它的凭证版本信息登记公共密钥、凭证和 web 服务器的地址，它们是按照相应的由 web 服务器交付的数据周期地修正的。在步骤 312，移动台相应于用户的请求来请求和 web 页连接，以接收电子文件。这个请求是通过用于请求电子文件可以访问个人/秘密信息的 “得到(GET)”命令直接发送给 web 服务器的。这时，业务服务器不对正被发送给 web 服务器的 GET 命令进行

任何的附加处理操作，这里，web 服务器可以是一个银行服务器、一个股票交易服务器等等。

在步骤 314，当从移动电话接收到请求时，被请求连接的 web 服务器决定要被加密的数据，然后通过业务服务器将结果通知给移动电话。要被加密的数据包括个人/秘密信息，例如一个口令和一个信用卡号。其它的数据例如用户的注册 ID、普通字符信息等等不需要加密，以便加密的数据数量可以减少。这是很有用的，因为和有线互联网通信相比，移动互联网通信要处理的数据的数量是很有限的。在步骤 316，业务服务器发送周期地由 web 服务器修正的目前登记的凭证版本给移动台。凭证版本提供可被用于确认消息源的关于 web 服务器的主机名、IP 地址和公共密钥的更新的信息。然后，移动台决定是否接收的凭证版本和先前登记的版本是一样的。先前登记的版本是由移动台从先前访问的相同的 web 服务器下载的。如果它们是一样的，用它先前登记的版本实现加密。

另一方面，如果是不相同的，移动台请求业务服务器发送一个新版本的凭证。这个请求是由“CERT”命令进行的，它是在移动台和业务服务器之间预先安排的用于发送凭证的协议。响应于命令“CERT”，在步骤 320，业务服务器发送目前登记的 web 服务器的凭证。亦即，如果有一个移动台对一个新的凭证版本的请求，具有周期地从 web 服务器上(内容服务器)下载的更新的信息的业务服务器(或代理服务器)发送一个响应消息，包括报头(header)和正文。在报头中，数字 SIGN(由移动台请求的 web 服务器的公共密钥签名)附于其中，凭证(主机名、IP 地址和公共密钥)附于正文部分。

在步骤 322，移动台接收来自业务服务器的响应消息，由验证在报头中的数字 SIGN 鉴别凭证的正文。即，移动台检查是否数字 SIGN 相应于 web 服务器的公共密钥，也检查是否正文被损坏。如果数字 SIGN 得到确认，移动台恢复被包含在凭证中的公共密钥，修正其中的其凭证表。在步骤 324，使用包含在凭证中的公共密钥，产生会话密钥，用于用户的信息安全传输。如上面所描述的，按照 128 位 SEED 算法产生会话密钥，它用于加密由移动台用户发送的个人数据。在步骤 326，用户的信息被会话密钥加密实现安全数据。在步骤 328，会话被公共密钥加密以产生对称密钥。

在步骤 330，由使用公共密钥加密会话密钥获得的对称密钥以及由会话密钥加密的数据经业务服务器被发送给 web 服务器，当然，业务服务器

不对正发送给 web 服务器的数据进行任何另外的操作，然后，在步骤 332，web 服务器使用保密密钥解密包含在从移动台接收的用户信息中的对称密钥，以产生一个会话密钥。在步骤 334，web 服务器使用产生的会话密钥解密用户信息，即，由移动台加密的安全数据，以便可恢复原始数据，从而原始数据可被 web 服务器处理。

同时，在步骤 320，使用散列函数产生一个散列值(即，消息文摘 5(MD5))。MD5 是用于加密的功能协议，其中如果结果与凭证相符，则认为数据传输已正常完成而没有任何外部的电脑黑客。对凭证的内容产生 128 位散列值(即，128 位字母序列)，用业务服务器的保密密钥加密，然后添加到凭证中。当移动台接收凭证时，移动台取加密的散列值，用业务服务器的公共密钥解密它。然后，为校验凭证还未被窃取，移动台再次产生凭证散列值且将它与解密的散列值比较，如果两者匹配，凭证是有效的。据此，一个安全的散列值用于认证消息，保证从业务服务器发送的数据在途中未被窃取，然后，校验 web 服务器的公共密钥有效，并执行步骤 324。

虽然先前的描述涉及从移动台发送给 web 服务器的用户信息，它也适用于需要安全性的用户信息的相反的传输。在这种情况下，移动台同样可以使用公共密钥和保密密钥解密来自 web 服务器的加密的信息。

此外，用于移动台和 web 服务器的安全交易应用程序被如下面所描述的那样准备。

首先，用于通过加密/解密保护用户信息的 HTML 文件被准备和上载给 web 服务器。通过使用在互联网协议中定义的类属性，由互联网搜索引擎区分需要加密/解密的 HTML 文件和普通 HTML 文件。这可通过指定类为安全指示符“SCURE”来实现，它表示要被加密的相应字段。

因此，本发明提供一个装置，用于在移动互联网中保密用于电子贸易的用户信息。

虽然本发明连同实施例伴随附图已加以描述，对那些在本领域中的普通技术人员来说是很清楚，可以进行各种变化和修改而不脱离本发明的宗旨。

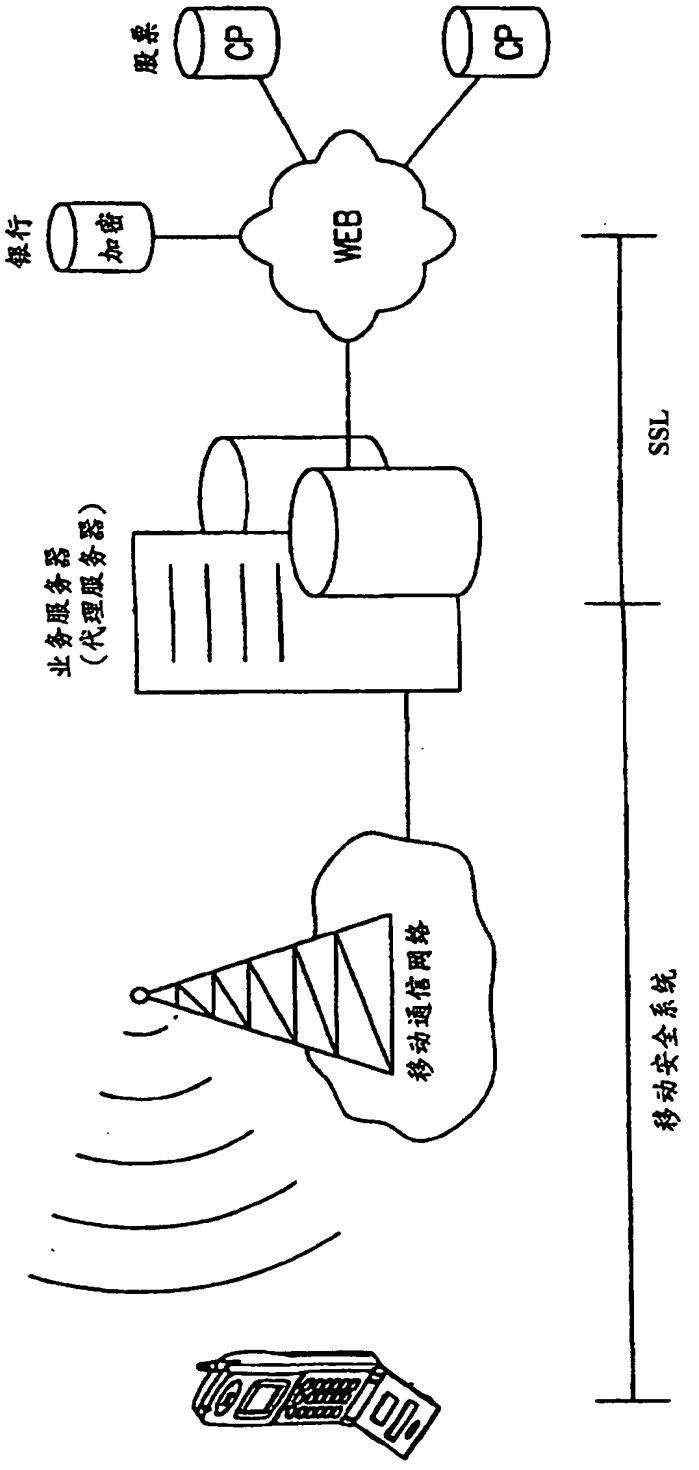


图 1

图 2

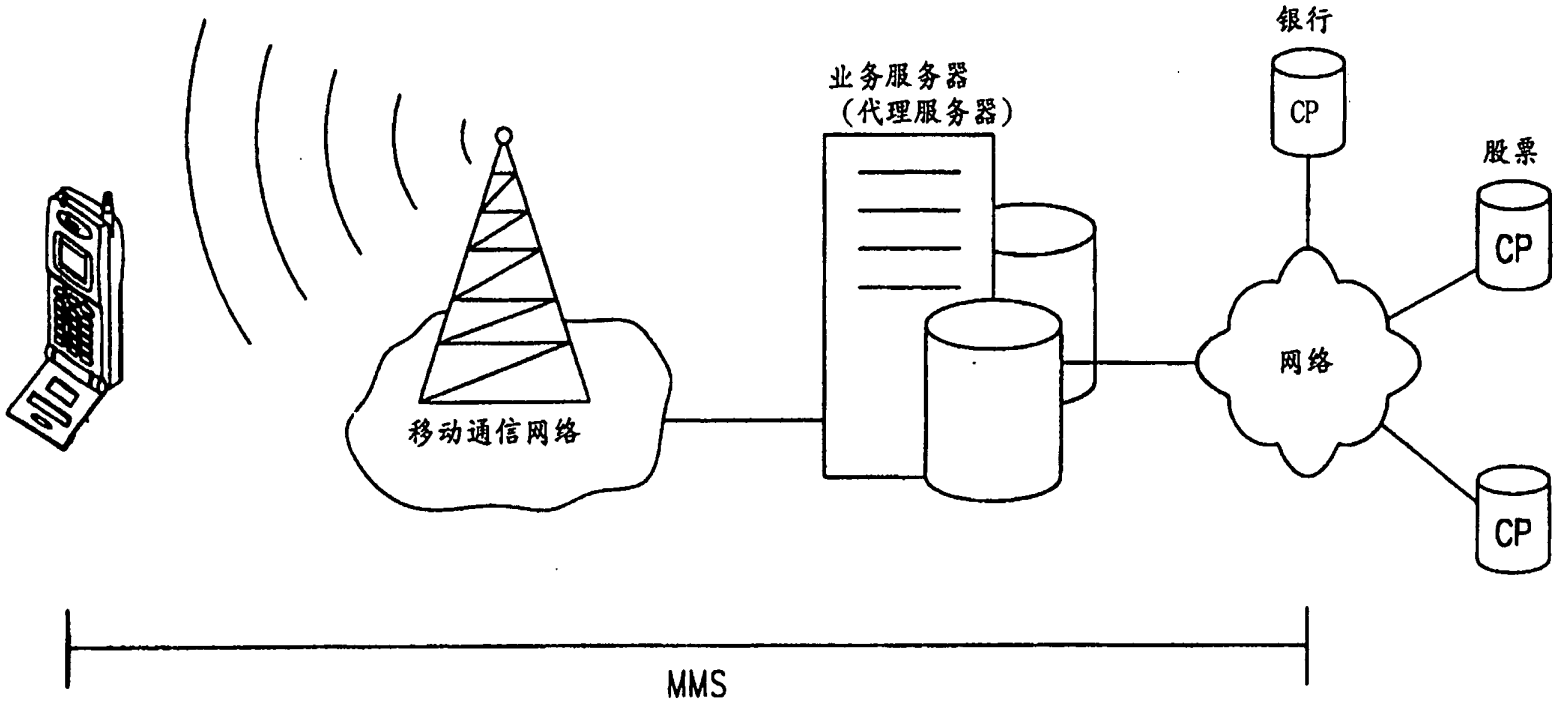
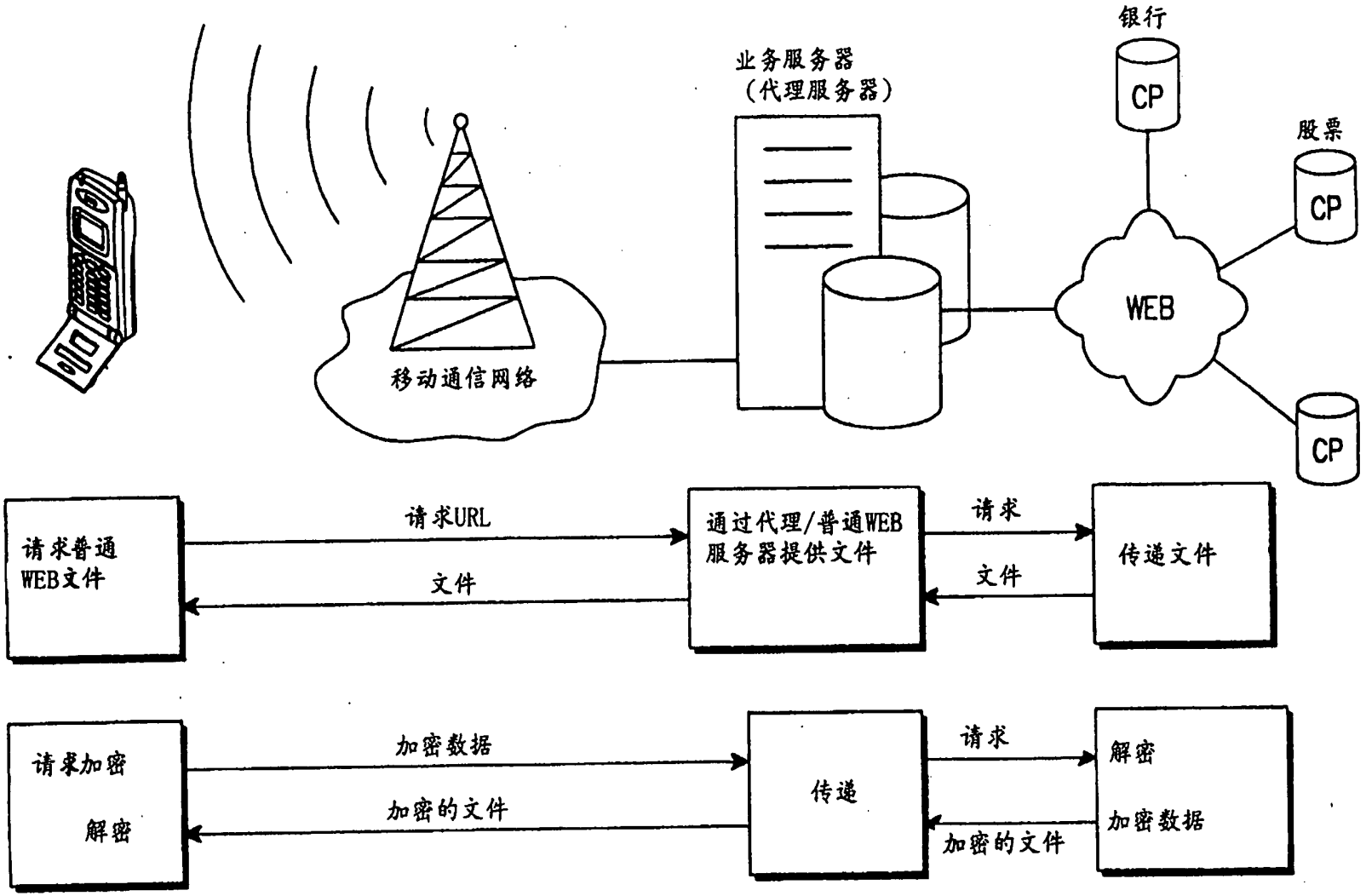


图 3


银行
业务服务器
（代理服务器）
CP
股票
CP
WEB
CP
移动通信网络
请求普通
WEB文件
请求URL
文件
通过代理/普通WEB
服务器提供文件
请求
文件
传递文件
请求加密
解密
加密数据
加密的文件
传递
请求
解密
加密数据
加密的文件

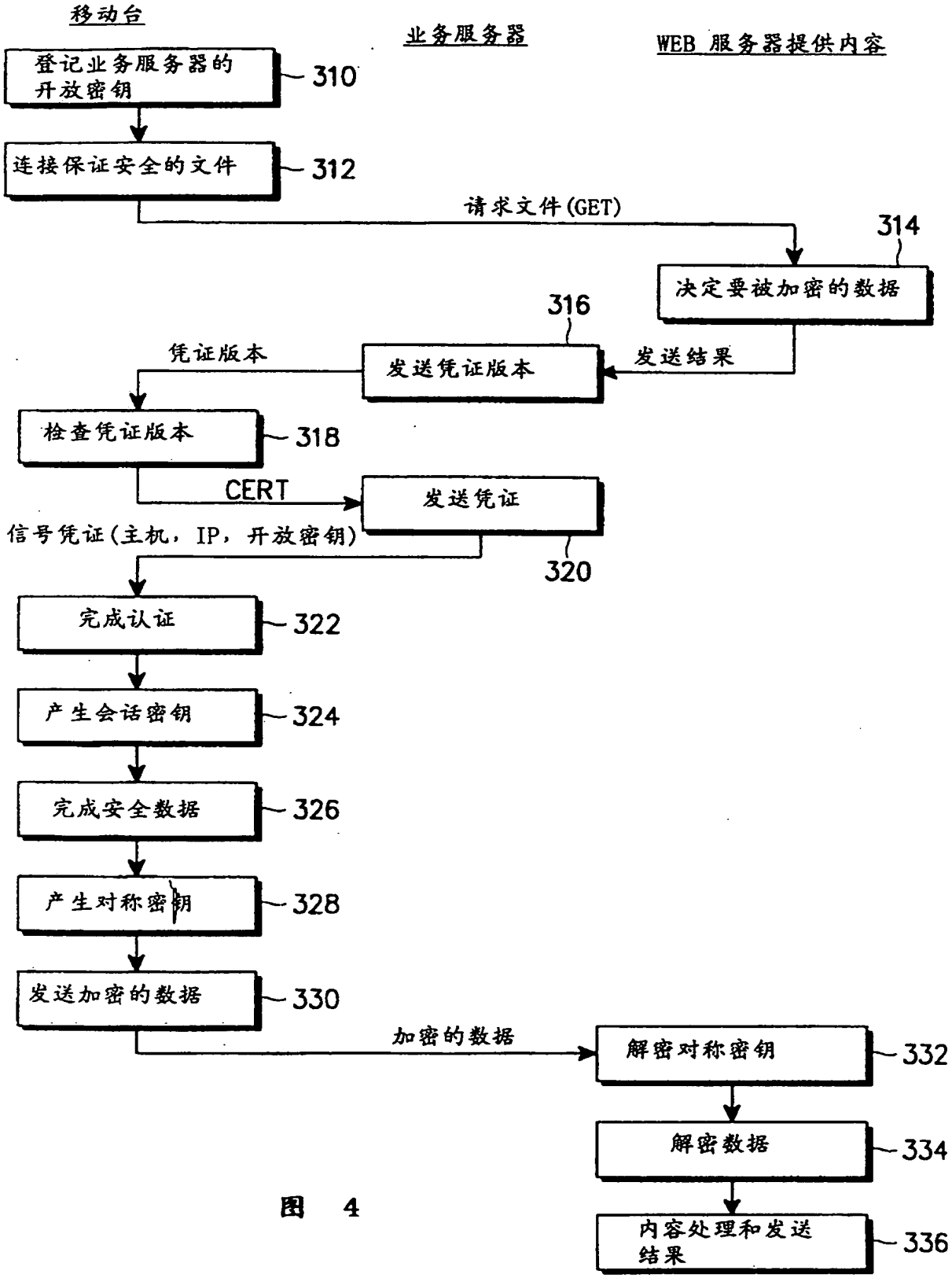

移动台
业务服务器
WEB 服务器提供内容
登记业务服务器的开放密钥
310
连接保证安全的文件
312
请求文件(GET)
314
决定要被加密的数据
316
发送凭证版本
发送结果
凭证版本
检查凭证版本
318
CERT
发送凭证
信号凭证(主机，IP，开放密钥)
320
完成认证
322
产生会话密钥
324
完成安全数据
326
产生对称密钥
328
发送加密的数据
330
加密的数据
解密对称密钥
332
解密数据
334
内容处理和发送结果
336

图 4